IMPORTANCIA DE LA GESTIÓN CENTRALIZADA DE REGISTROS EN UN CORRELACIONADOR DE EVENTOS (SIEM) EN UNA ORGANIZACIÓN

Cómbita Hernández Juan Pablo
jcombita10@hotmail.com
Universidad Piloto de Colombia

Resumen—En este trabajo se explica la importancia del SIEM o correlacionador de eventos mostrando los orígenes, la evolucionado hasta el día de hoy; Como funciona, los dispositivos que se pueden registrar para él envió de eventos, métodos y la clasificación de los mismos, todo esto aplicable a una organización en cualquier sector de la industria.

Abstract—This paper explains the importance of the SIEM or correlator of events showing the origins, the evolution to this day; How it works, the devices that can be registered for the sending of events, methods and their classification, all applicable to an organization in any sector of the industry.

Índice de términos—Correlacionador, eventos, Organización y SIEM

1. INTRODUCCIÓN

Las organizaciones de hoy en día cuentan con aplicaciones, servidores con sistemas operativos y herramientas, que generan registros de eventos de seguridad, llamados logs, estos contienen información acerca de los sucesos que ocurren en el dispositivo.

Es importante mantener un monitoreo constante de los logs para detectar eventos anormales en las herramientas o dispositivos de red, y poder actuar oportunamente frente a cualquier dificultad, evitando así la pérdida o manipulación no autorizada de información. Sin embargo, no es suficiente analizar la información de cada dispositivo por separado, ya que, en algunos casos, puede existir una relación directa entre eventos sucedidos en distintos equipos. La revisión de los logs y análisis de la información contenida en éstos se vuelve una tarea bastante compleja si tenemos en cuenta que por segundo se pueden generar infinidad de eventos por las distintas maquinas. Una solución a éste problema es mantener almacenados los logs en un solo equipo, y desde este hacer la revisión de todos los logs de la organización.

Existen algunas herramientas de software que permiten realizar la centralización de los registros de eventos y en algunos casos correlacionarlas, se encuentran herramientas de código libre o guías que permiten realizar el transporte sobre los logs, pero no cumplen con todos los requerimientos de seguridad necesarios para el transporte de estos.

Los Correlacionadores de eventos o security information and event management (SIEM) – recogen, analizan y priorizan los eventos de seguridad dentro de su red. Existen varios tipos de soluciones, desde los colectores de logs hasta las soluciones más completas, que ayudan a implantar SIEM de acuerdo con las "mejores prácticas" en cumplimiento de las normativas y estándares de seguridad más exigentes.

2. ORIGEN DE LOS SIEM Y CONDICIONES GENERALES

Las soluciones SIEM son una combinación de las categorías de productos formalmente dispares SIM (security information management) and SEM (security event manager). La tecnología SIEM proporciona un análisis en tiempo real de las alertas de seguridad generadas por el hardware y software de red. Las soluciones SIEM pueden venir como software, appliance, o administración de servicios, y también son utilizados para loguear datos de seguridad y generar reportes para fines de complimientos.

Un sistema SEM centraliza el almacenamiento y la interpretación de los registros y permite un análisis casi en tiempo real que permite al personal de seguridad tomar medidas defensivas más rápidamente. Un sistema SIM recopila los datos en un repositorio central para el análisis de tendencias y proporciona informes automatizados para el cumplimiento y la generación de informes centralizados. Al unir estas dos funciones, los sistemas SIEM proporcionan una identificación, un análisis y una recuperación más rápidos de los eventos de seguridad. Esto también permite a los administradores de cumplimiento confirmar que están cumpliendo con los requisitos de cumplimiento legal de una organización.

Los sistemas SIEM son típicamente caros para desplegar y son complejos de operar y administrar. Mientras que el cumplimiento del estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) ha impulsado tradicionalmente la adopción de SIEM en grandes empresas, las preocupaciones sobre amenazas persistentes avanzadas han llevado a las organizaciones más pequeñas a considerar los beneficios que ofrece un proveedor de servicios de seguridad administrada por SIEM. La enorme cantidad de registros, eventos y flujo de datos en soluciones

SIEM, ofrece a los analistas de seguridad respuestas a preguntas esenciales tales como "¿quién está accediendo a los sistemas de negocios?", o, lo que es más importante, "¿hubo alguna actividad extraña antes, durante o después de la conexión?", Sin embargo, para obtener las respuestas a estas preguntas los usuarios necesitan filtrar, correlacionar, y ver los eventos relevantes del sistema SIEM, agregando "contenido" al propio sistema. Normalmente, el experto de SIEM crea y mantiene la gran cantidad de visualizaciones de panel, reglas de correlación, listas de vigilancia, alarmas, e informes relacionados con este procesamiento de datos para extraer información de eventos y desde luego, casos de uso. Por ejemplo, crear reglas de correlación no sólo requiere de un conocimiento a fondo de la actividad del adversario, sino también un conocimiento del sistema de datos SIEM para crear el contenido adecuado sin afectar el desempeño del mismo. La combinación requerida entre el conocimiento de amenazas y la configuración del sistema, puede llevar mucho tiempo y puede ser una labor desafiante antes de que se obtenga el desempeño total de la solución SIEM.

Las guías sobre el uso, los tipos de dispositivos relacionados y los pasos de pre y post instalación se explican por lo general por parte del proveedor de la herramienta (Tenable, Splunk, Mcafee, ect), al administrador del sistema para obtener mejor conocimiento y resultados. Después de la instalación, la mayoría del contenido, que incluye informes y reglas de correlación, se pueden adaptar a entornos empresariales específicos de usuario. La distribución de los paquetes de contenido se proporciona mediante la solución escogida ya que por defecto estas tienes reglas establecidas por defecto y lo que se debe es afinar de acuerdo al objetivo y necesidades de la organización, también es de tener en cuenta que depende del segmento en el cual se ubique la herramienta para solicitar los permisos de firewall según sea la necesidad.

A continuación, se va a explicar algunos puntos débiles de las soluciones SIEM

La gran mayoría de las soluciones SIEM tienen demasiados datos inútiles no estructurados, un claro ejemplo son el gran número de entradas de registro para cada cambio ejecutado en los datos y configuraciones del sistema. Por este motivo, encontrar la causa o solucionar urgentemente un incidente de seguridad no será posible ya que llevará mucho tiempo y esfuerzo analizar toda la información.

En los SIEM los informes que son generados ante eventos o cambios son incompletos en caso de incidente de seguridad, en algunos casos es imposible analizar los datos antes y después del incidente, por lo que estos estos informes no contienen información relevante sobre los objetos modificados o eliminados. Informes difíciles de comprender ya que no dejan claro quién ha cambiado qué, cuándo y dónde dentro de la organización. Las Crecientes amenazas cambiantes y persistentes internas contra los recursos de TI como: Bases de datos, servidores de correo, etc. en las cuales, de no tenerse un afinamiento de las políticas en los dispositivos de red como Firewall, switch, routers, etc, las reglas del SIEM empezaría a generar un gran volumen de alertas, por esta razón se deben ajustar políticas de seguridad cuando crece el riesgo basado en evidencias o incidentes ya comprobados. En la mayoría de SIEM no es fácil buscar y descubrir evidencias o temas de ingeniería forense ante una eventualidad o suceso informático. Malware en la infraestructura que puede generar DDos, Dos (denegación de servicios sencillo o distribuido).IPS/IDS generan muchos falsos positivos.

Cuando se presenta un incidente no hay forma de reconstruir posible evidencia en forma correlacionada.

3.MÉTODOS DE TRANSPORTE

Existen diferentes métodos que se pueden utilizar a la hora de realizar el transporte de los logs al correlacionador. A Continuación, se describen algunos de estos.

3.1. Syslog

"*Syslog es un sistema de logs que se encarga principalmente de la administración de logs, los cuales son generados por eventos del sistema, sus programas o por el Kernel.*" ***[1]***

El envió de mensajes syslog fue usado inicialmente en sistemas basados en UNIX para registrar eventos de aplicaciones, sistema operativo o red. Es común ahora encontrar equipos de redes que pueden generar y enviar mensajes syslog a equipos configurados con un demonio que los reciba, así como ya existen implementaciones para sistemas Windows.

"El termino syslog es a menudo utilizado para describir tanto el protocolo para el envío de mensajes, como el programa o librería que envía mensajes syslog". ***[2]***

Es de tener en cuenta que Syslog utiliza el protocolo UDP, este protocolo es no orientado a conexión por lo cual no se asegura que los mensajes lleguen al destinatario. Los mensajes que viajan por la red no están cifrados y viajan como texto plano por lo cual se convierten en susceptibles a ser vistos por personas no autorizadas; Incluso cualquier persona puede dirigir mensajes de una naturaleza maliciosa, sin ninguna autenticación de quien es el remitente lo que puede concluir en ataques de denegación de servicios permitiendo que un atacante distraiga al administrador con mensajes falsos para no llamar la atención con su ataque.

En resumen, podríamos decir que éste protocolo presenta desventajas en cuanto al manejo de seguridad ya que no garantiza la llegada del mensaje al utilizar un protocolo no orientado a conexión, ni tampoco garantiza integridad, autenticidad, ni confidencialidad.

3.2. SNMP

SNMP (Simple Network Managment Protocol) es un protocolo de administración de red, que gestiona la configuración de dispositivos de red desde una estación de trabajo. Sin embargo, existen algunos dispositivos de red

que no fueron creados para ser administrados con SNMP, para lograr la administración de estos existe un agente especial llamado agente Proxy. SNMP v.1 trabaja con el protocolo de transporte no orientado a conexión, UDP. Los agentes SNMP escuchan por el puerto 161.
SNMP ha evolucionado actualmente se encuentra en la versión 3 que se define como la adición de seguridad y administración a SNMP v.2.
Esta versión fue diseñada para corregir, mediante el uso de algoritmos de autenticación y de cifrado, algunos problemas de seguridad con los que contaba la versión 2, falta de Integridad, Autorización, Autenticación y se presentaba spoofing, sin embargo, aún no previene ataques como denegación de servicios y sniffer,
La versión 3 utiliza un cifrado por medio de DES y autenticación con MD5. También utiliza un modelo de usuarios y de control de acceso basado en vistas sobre la Base de Información Gestionada (MIB), esto permite que se pueda restringir el acceso a ciertas partes de la MIB.
Otra mejora de esta versión frente a las versiones anteriores, es que soporta el uso de lenguajes orientados a objetos, como Java o C++, para la construcción de los elementos propios del protocolo.
Hay que hacer especial referencia, nuevamente, adelantos en el tema de seguridad garantizando integridad, autorización, autenticación y spoofing; este protocolo se puede ver como una herramienta útil en la administración de logs.
No basta con transportar los registros de eventos a un punto central, se debe garantizar que el transporte cumple con los requerimientos que obligan a tener un mecanismo que garantice la autenticación, integridad y confidencialidad.

4.CORRELACIÓN DE REGISTRO DE EVENTOS DE SEGURIDAD

La correlación tiene como objetivo encontrar incidentes los cuales son una serie de eventos que ocurren en distintos puntos de la red y la correlación busca la asociación de dichos eventos para encontrar información que nos aclare cuál fue el origen del incidente.
Para realizar una correcta correlación es necesario cumplir requisitos como Consolidación, Normalización y Reducción:La consolidación de los datos consiste en el transporte de los eventos desde los dispositivos o herramientas de seguridad hasta el punto central. El método de transporte que se utilice debe ser orientado a conexión y nos debe garantizar principios básicos de seguridad como integridad y disponibilidad, por lo cual se debe proteger los datos durante el transporte, para lo cual se debe utilizar algún método de cifrado y autenticación.La normalización de los datos consiste en cambiar el formato de los datos a un solo formato estándar, que sea interpretado por el SIEM ya que en caso de que se necesite realizar una imagen forense durante el proceso no se cambie ningún dato.La reducción de los datos para comprimir información que nos permite almacenar y transportar más información, sin que este duplicada o combinando eventos similares en uno solo.
Teniendo en cuenta que uno de los aspectos más importantes de un registro de eventos es guardar el registro de tiempo exacto del momento en que se produjo el log y a la hora de correlacionarlo, como son varios eventos los que se tendrán y de varios dispositivos, se puedan sincronizar.
Es importante que los logs de la información que se correlaciona cumpla con requisitos de normalización, sincronización de tiempo, transporte y reducción para lograr una correlación exitosa.

4.1. Eventos Primitivos y Compuestos

Un incidente lo definimos como el resultado de la correlación de varios eventos.

"la correlación…, es tomar varios eventos de seguridad aislados y unirlos para crear un único y relevante incidente de seguridad.". ***[4]***

Un evento es un cambio que ocurre en un sistema presentado por un factor que no corresponde a lo usual del sistema. Se clasifican en eventos primitivos y compuestos.
Eventos primitivos se encuentran predefinidos en un sistema y la detección esta embebida en la implementación del sistema.
Eventos compuestos surgen de componer varios eventos primitivos que se pueden producir de manera recurrente.
Se ha definido un lenguaje para especificar eventos compuestos llamado JESL (Java Event Specification Languaje) que se compone de la siguiente manera.

- Evento
- Evento Primitivo
- Evento Compuesto
- Instancia de Evento (intervalos de recurrencia de eventos)

Estos eventos al momento que se correlacionan se tienen en cuenta aspectos importantes como la velocidad de correlación y la exactitud de los datos devueltos en la correlación. Es importante que el sistema de correlación devuelva los resultados lo más pronto posible para que el oficial de seguridad o persona encargada de la revisión de eventos del correlacionador pueda actuar, es importante tener en cuenta que el correlacionador debe reducir el número de falsos positivos y falsos negativos.

4.2. Métodos de correlación

La correlación se puede realizar mediante varios métodos correlación basada en reglas, correlación estadística y correlación con sistemas de inteligencia artificial. Correlación basada en reglas consiste en identificar ciertos incidentes y su secuencia, cada uno de los eventos que se dieron para llegar al incidente, a ese tipo de conocimiento de ataque se le utiliza para relacionar eventos y analizarlos en un contexto común. Los motores de correlación basados en reglas aplican los incidentes conocidos en un ataque para seguir detectando exactamente el mismo ataque, o sea los sistemas basados en reglas combinan un conjunto de reglas con los eventos que van recibiendo y las combinaciones de los mismos, basándose en los resultados de cada prueba y el

conjunto de reglas configuradas, el motor de procesamiento de reglas analiza los datos obtenidos hasta que llega a un estado final el cual es reportado en un diagnóstico.

Es muy importante tener en cuenta en este método que para que la correlación funcione bien y los resultados sean exactos, que las reglas que se configuren sean precisas, concisas según los sistemas o aplicaciones y actualizarlas en caso de algún cambio en los datos.

Correlación estadística consiste en que no se emplea ningún conocimiento ya existente de incidentes, sino que por el contrario confía en el conocimiento de actividades normales del sistema o aplicación que se han acumulado en un cierto tiempo, luego, los eventos en curso son clasificados por un algoritmo incorporado y se pueden también comparar a los patrones acumulados de la actividad, para diferenciar eventos normales de sospechosos o diferentes.

La correlación estadística utiliza algoritmos numéricos especiales para calcular los niveles de amenaza incurridos por los elementos relevantes de la seguridad, esta correlación busca desviaciones de niveles normales de eventos y otras actividades rutinarias. Los niveles de riesgo se pueden calcular de los eventos entrantes y seguir posteriormente en tiempo real o históricamente, de modo que las desviaciones lleguen a ser evidentes.

Es muy importante tener en cuenta en este método que la detección de incidentes no requiere ningún conocimiento preexistente del incidente a ser detectado, se puede utilizar este método para detectar incidentes en umbrales definidos de la actividad.

Correlación con sistemas de inteligencia artificial utilizan varias técnicas como lo son redes neuronales y sistemas expertos. Cuando están bien programados los sistemas de inteligencia artificial están en la capacidad de aprender por si solos, ayudando a eliminar la necesidad de los expertos. Este tipo de correlación se basa en la forma que el cerebro humano realiza correlación de información

4.3. Métodos de conservación de la información

La información se debe saber conservar, almacenar ante posibles eventos en los cuales se materialice el riesgo de pérdida de información y sea necesario una investigación forense, esta ciencia se encarga de crear y emplear medidas preventivas para eventos ocurridos en sistemas de información.

La ingeniería forense también asiste en la reconstrucción posterior de eventos para esclarecer las posibles causas y/o métodos de posibles pérdidas por las cuales se cometió un delito informático, esta información serviría como evidencia para un posible asunto legal complemento para las pruebas de un abogado.

El uso del análisis forense y la evidencia digital nos ayuda a identificar y poder procesar los delitos informáticos, los expertos en forense utilizan técnicas y herramientas de software que ayudan en el proceso de análisis computacional.

Una investigación forense comienza con la recolección de datos que estén presentes en el sitio del incidente, esta información a recolectar debe ser tomada con ciertas técnicas para que las evidencias recolectadas no atenten contra los pilares de la seguridad informática, es de tener en cuenta que si la evidencia se recolecta para un proceso judicial es mal recolectada sin estándares, ni técnicas no es válida. **[5].**

En una organización si se llega a presentar un incidente de seguridad una principal fuente de información de la cual se puede recolectar es el correlacionador de eventos, ya que, al estar integrado con todos los servidores y aplicaciones, en el SIEM podemos ver trazabilidad de los inconvenientes de las mismas y tener un referente de donde podemos continuar con la investigación.

En los incidentes de seguridad las personas involucradas, por lo general, intentan manipular y alterar la evidencia digital, tratando de borrar cualquier rastro que pueda dar muestras del daño, por esto es importante tener un correlacionador con buenas políticas de seguridad y registro ya que con esto aseguramos la trazabilidad de la información, es bueno también mitigar estos posibles problemas con recolección de evidencia digital por:

La evidencia digital al ser recolectada puede ser duplicada de forma exacta y se puede sacar una copia para ser examinada como si fuera la original, esto se hace por lo general para evitar el riesgo de dañar la información original.

La ingeniería forense actual está en capacidad por medio de las herramientas y técnicas comparar la evidencia digital con la original y determinar si esta evidencia digital ha sido alterada.

La evidencia digital es difícil de eliminar, así la información se halla borrado del disco duro, y este incluso haya sido formateado, por medio de las técnicas forenses es posible recuperar esta información.

La evidencia digital la podemos clasificar en:

Registros generados por el computador, estos son los registros que son generados por la misma máquina y son inalterables por el ser humano, estos registros llamados logs almacenan los eventos de seguridad del pc y sirven para demostrar el correcto y adecuado funcionamiento del sistema.

Registros no generados por la maquina sino simplemente almacenados por o en la computadora. En estos registros es importante poder demostrar la identidad del generador probando los hechos o afirmaciones contenidas en los posibles documentos generados humanamente y que se van a considerar como evidencia.

Registros híbridos que incluyen registros almacenados en logs y registros generados humanamente, estos son los registros que combinan logs con archivos creados por una persona.

Es de tener en cuenta que también existen unos criterios de admisibilidad al momento de empezar a evaluar la evidencia y que está tenga un valor judicial en caso de ser necesario, los criterios en cuestión son:

Autenticidad: una evidencia digital se puede considerar autentica si cumple que dicha evidencia ha sido generada y registrada en el lugar de los hechos y que se pueda demostrar que los medios originales no han sido

modificados y corresponden efectivamente y son un fiel reflejo de la realidad. Es importante tener en cuenta que en los medios digitales se presenta un alto grado de manipulación, por esta razón se debe verificar la autenticidad de las pruebas presentadas en medios digitales, contrario a las no digitales, en las que la autenticidad de las pruebas no será puesta en duda de acuerdo con lo dispuesto en el artículo 11 de la ley 446 de 1998:

"Autenticidad de documentos. En todos los procesos la autenticidad de documentos privados presentados por las partes para ser incorporadas a un expediente judicial con fines probatorios, se reputarán auténticos, sin necesidad de presentación personal ni autenticación. Todo ello sin perjuicio de lo dispuesto en relación con los documentos emanados de terceros" ***[6]***

Para asegurar el cumplimiento de la autenticidad se requiere que una arquitectura exhiba mecanismos que certifiquen la integridad de los archivos y el control de cambios de los mismos.
Confiabilidad: los registros de eventos de seguridad son confiables si los orígenes son creíbles y verificables. Para probar la confiabilidad se debe contar con una correcta implementación de reglas del SIEM, en lo cual se demuestra que los logs que se generan tiene una forma confiable de ser identificados, recolectados, almacenados y verificados.
Una prueba digital es confiable si:

"La prueba digital debe ser adquirida del modo menos intrusivo posible, tras un proceso que sea trazable y auditable, tratando de preservar la utilidad y originalidad de la prueba. Ese proceso debe ser reproducible, comprensible y verificable, y para ello las herramientas utilizadas deben ser contrastadas." **[7]**

Las reglas configuradas en el correlacionador deben ser precisas para todos los dispositivos validando que las horas, tanto del SIEM como del correlacionador son las mismas según el protocolo NTP (Network Time Protocol), protocolo de internet que se utiliza para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable. Para la instalación y configuración de NTP es necesario determinar un servidor de NTP **[8].**
Si el sistema operativo es Linux debe contar con sistema operativo Unix-Like y si es Windows contar con el protocolo SNTP mínimo versión 2. Si son dispositivos de red (routers, switch, etc), deben también sincronizarse y deben correr el protocolo NTP o SNTP.
Para realizar una correcta manipulación de la evidencia digital se debe tener en cuenta.
Aplicar una correcta ingeniería forense con respecto a la forma como se debe recolectar la información teniendo en cuenta la aplicación con la cual la vamos a realizar.
Mantener y controlar la integridad del medio original, o sea que cuando se vaya a recolectar la información que nos va a servir de evidencia digital, las acciones realizadas no deben modificar la evidencia tomada.
Las personas que pueden tener acceso a la evidencia digital debe ser un profesional forense para no alterar o dañar la evidencia tomada.
Las copias que se saquen de la evidencia original deben estar controladas, marcadas y preservadas teniendo en cuenta que los resultados de la investigación deben estar disponibles para una revisión por parte de una persona competente legalmente o con la experticia en seguridad de la información.
Cuando la evidencia digital se encuentre en poder de una persona, este será el responsable de todas las acciones tomadas con respecto a ella mientras esté en su poder.
Las agencias u oficiales de seguridad responsables de llevar el proceso de recolección y análisis de la evidencia digital, serán quienes deben garantizar el cumplimiento de los anteriores principios.

4.4. Protección de información y herramientas de seguridad que le reportan al correlacionador de eventos

Es importante tener en cuenta las técnicas existentes para proteger la información y los recursos de una red, en los cuales va estar incluido nuestro correlacionador de eventos ya que éste va a recibir los eventos de estos dispositivos. Estas técnicas las podemos clasificar en seguridad física y seguridad Lógica.

4.4.1 Seguridad física: la seguridad física es uno de los aspectos más importantes durante el diseño de un sistema de seguridad informática ya que se refiere a controlar e implementar mecanismos de seguridad dentro y alrededor del centro de cómputo o instalaciones en las cuales se encuentren servidores o mainframes que contengan la información de importancia para la organización, esto también incluye los mecanismos de seguridad en los medios de acceso remoto al centro.
La importancia de implementar estos mecanismos de seguridad es proteger el hardware y los medios de almacenamiento de datos, incluyendo las instalaciones físicas, ya que no se está exento de las amenazas de la naturaleza (desastres naturales, incendios accidentales, terremotos, inundaciones, etc.), o las ocasionadas por el mismo hombre (atentados terroristas, disturbios, sabotajes internos y externos).

4.4.2 Seguridad lógica: este tipo de seguridad tiene como función la imposición de barreras y procedimientos que protejan el acceso a los datos y solo se permita acceder a ellos a los usuarios autorizadas para hacerlo, asegurando con esto los principios de la seguridad (integridad, confidencialidad y disponibilidad), también se debe verificar que la información (confidencial) que sea trasmitida se reciba solo por el destinario al cual ha sido enviada, asegurando que la información recibida sea la misma que ha sido trasmitida.

4.4.3 Protección: la mayoría de los problemas se seguridad son ocasionados por los usuarios de los sistemas y es responsabilidad del administrador detectarlos y encontrar la mejor manera de terminar con ellos, es importante tener en cuenta que cualquier dispositivo de seguridad no es 100% confiable pero que una buena configuración de reglas y políticas en todos los dispositivos de la red forman una buena barrera, se van a explicar algunas técnicas de protección que con la suma de ellas se convierte el sistema interconectado en un medio confiable.

4.4.3.1 Criptografía: es una técnica que permite mantener la información en modo privado y protegido con lo cual se impide que un externo permitido a la información la pueda ver en claro. Al tener cifrada la información que se envía por la red se garantiza que no sea la información real, sino que se encuentra codificada y carente de sentido excepto para el receptor quien cuenta con los medios precisos para decodificarla.
La criptografía nos ayuda para proteger la confidencialidad de la información. Su objetivo principal es dificultar el ingreso a la información por parte de un usuario no autorizado, inclusive si este posee la información cifrada y conoce el algoritmo de cifrado utilizado. Algunos de los métodos más usados actualmente para esta técnica son la criptografía simétrica, la criptografía asimétrica y la criptografía hibrida que es la combinación de las los anteriores; Estos métodos son basados en el manejo de llaves privadas y públicas combinados con funciones matemáticas.
Simétricos: se utiliza una clave igual para cifrar y descifrar la información lo que permite su fácil implementación y ejecución, la desventaja de este algoritmo es que no proporciona autenticación.
Asimétricos: se utiliza clave diferente para la llave pública y privada relacionadas entre sí, en donde la información cifrada por la primera de ellas solamente puede ser descifrada por su par y viceversa. Con este tipo de algoritmo si obtenemos confidencialidad y autenticación.

4.4.3.1 Autenticación: esta técnica se refiere al proceso de verificar la identidad de una persona, por medio de sistemas biométricos como la huella digital, firmas digitales, passwords, smartcadrs, certificados, etc.

4.4.3.2 Firewalls (FW): es un sistema que ejerce políticas de seguridad establecidas. Este sistema puede ser de software ejecutándose en un sistema operativo o en un enrutador o puede ser hardware. El firewall puede proteger una red confiable de una que no lo es como es el caso de la internet. Los FW son utilizados para controlar el tráfico de paquetes entrantes y salientes entre redes internas o externas de distintos segmentos de red, si el tráfico es anormal o extraño el FW le restringe el paso.
4.4.3.3 Listas de control de acceso (ACL): son las listas que permiten definir permisos a usuarios y grupos concretos. En una organización es muy común que se defina sobre un Proxy una lista de todos los usuarios que tienen permisos a servicios como SMTP, SFTP, FTP, etc., incluso a internet. También se puede definir limitaciones de ingresos de uso del ancho de banda entre otros.

4.4.3.4 Sistemas de detección de intrusos (IDS): estos sistemas son diseñados para examinar el tráfico que viaja por la red con el fin de identificar amenazas y a la vez detectar escaneos no autorizados y posibles ataques.
Los IDS también controlan logs para descubrir anomalías de intrusos o usuarios no autorizados, también mantienen almacenado el estado exacto de archivos del sistema para detectar la modificación de los mismos. Se utilizan dos métodos de detección
Por firmas: en el cual el IDS busca patrones predefinidos dentro del tráfico.
Por anomalías: el IDS busca desviaciones si observa algo anormal en la caracterización del tráfico y estadísticas del sitio.
La desventaja de los IDS es que en ocasiones arroja resultados denominados falsos positivos que son alertas que se reportan pero que cuando se observa el reporte y se realiza el análisis del caso la información reportada no tiene ningún malware o anomalía.

4.4.3.5 Antivirus: es un programa creado a base de firmas que se actualiza con cierta regularidad para prevenir la penetración de virus en un equipo, evitando su propagación por los distintos dispositivos de red (servidores, estaciones de trabajo y dispositivos que funcionen bajo un sistema operativo), es de tener en cuenta que los malware (virus, troyanos, bombas lógicas, etc), atacan sistemas operativos comunes como Windows y Linux porque son los que más utilizan los usuarios.

4.4.3.6 Dispositivos de red: son los dispositivos que pueden enrutar paquetes analizándolos hasta cierta parte caso de los Switch, Router, Datapower entre otros. Algunos de estos dispositivos pueden ser configurados para generar alertas en caso de intentos de fuerza bruta.
Los enrutadores pueden realizar también tareas de control de ancho de banda y evitar de esta manera ataques de denegación de servicios.

4.5. Clasificación de eventos en el correlacionador
Se pueden clasificar los eventos alertados en el correlacionador de eventos en vulnerabilidades, amenazas y ataques, observemos cada uno:

4.5.1 Vulnerabilidades: es la posibilidad de que el sistema u organización este expuesto a una amenaza, las vulnerabilidades son un punto crítico de seguridad pueden ser aprovechadas por un atacante para acceder a un sistema o una red. Es bueno tener en cuenta que la gran mayoría de las vulnerabilidades se deben a malas configuraciones de los sistemas operativos, las aplicaciones y dispositivos de red, y también de la falta de conciencia de los usuarios a realizar las actualizaciones recomendadas por los fabricantes de software.

4.5.1.1 Tipo de vulnerabilidades: a continuación, se enumeran algunas de las vulnerabilidades más comunes.
DoS: la denegación de servicios es cuando el atacante intenta evitar que un usuario tenga acceso a la red, recursos o información y esto lo logra con un programa repetitivo que acceda a la aplicación saturando los puertos disponibles con múltiples conexiones consumiendo el ancho de la red de la víctima.
Stack Overflow: esta vulnerabilidad sucede cuando el tamaño máximo de la pila del sistema es excedido puede ser generado por un malware.
Path Manipulation: esta vulnerabilidad se presenta cuando se manipula el path de las aplicaciones, con lo cual se indican ubicaciones distintas y por lo tanto recursos distintos a los que se utilizarían normalmente.
Heap Overflow: en esta vulnerabilidad se utiliza el heap que es una región de memoria que se inicializa dinámicamente para un programa. Se realiza un heap overflow sobrescribiendo el contenido del heap con posible código malicioso o código arbitrario y sin límite en el componente del programa.
Commands inyection: esta vulnerabilidad permite al atacante introducir código dañino por medio del servicio web a otros sistemas a través de scripts y/o el protocolo http
Cross-site scripting: esta vulnerabilidad consiste en que el atacante redirige al usuario de una URL de un web server legitimo a uno con código HTML con Malware para posible robo de información.
SQL Injections: esta vulnerabilidad hace referencia a una técnica de explotar las aplicaciones web que no validan la información suministrada por el cliente, para enviar consultas SQL maliciosas por medio de un campo o parámetro de la aplicación, con el fin de realizar modificaciones sobre las bases de datos cuando la que está en riesgo es una organización.

4.5.2 Amenazas y ataques: una de las consecuencias de las vulnerabilidades son las amenazas. Una amenaza es una condición del entorno que se puede presentar en el sistema de un usuario o en la red de la organización, dada una oportunidad puede darse lugar a que se produzca una violación de los principios de seguridad; Cuando se materializa este tipo de violación hablamos de un ataque.

4.5.2.1 Clasificación de ataques según el principio de seguridad violado: los ataques se pueden clasificar globalmente según el modo de acción los más comunes son:
Interrupción: este ataque consiste cuando el atacante ataca un recurso del sistema para dejarlo inoperable o no disponible para los usuarios, en este ataque se viola el principio de la disponibilidad, un ejemplo puede ser cuando saturan con solicitudes a un servidor de Base de datos o a un servidor de aplicaciones.
Intercepción: este ataque se da cuando un usuario no autorizado o atacante consigue acceso a un recurso al cual no debería tener permisos, en este ataque se viola el principio de la confidencialidad, debido a que en este ataque no se produce ningún tipo de alteración sobre los recursos, hablamos de una persona atacante entre el emisor de la información y el receptor de la misma que es quien observa los datos que viajan por la red entre las dos puntas.
Modificación: en este ataque el intruso al acceder al recurso lo modifica., en este ataque se viola el principio de la integridad y como su nombre lo indica es cuando se realizan cambios en la información que se esté almacenando en un servidor o la que viaja por la red y estos cambios son realizados por una persona no autorizada.
Inclusión: en este ataque el intruso desarrolla información falsa y la inserta en la aplicación o recurso a atacar, en este ataque se viola el principio de la autenticidad, y esta información fraudulenta al ser añadida a archivos o enviados a usuarios producen posibles fugas de información de los usuarios que utilicen las aplicaciones o reciben los mensajes.

4.5.2.2 Clasificación del ataque según su efecto: se pueden clasificar en ataques activos y pasivos y buscan el mismo fin robar información o denegar servicios:
Activos: este ataque sucede cuando el usuario intruso realiza alguna modificación en los datos de una aplicación o que estén disponibles por la red.
Pasivos: en este ataque el usuario atacante monitorea toda la información que va por la red, no la altera ni la modifica solamente escucha y analiza el trafico pasante con la finalidad de interceptar la información que le resulte interesante posiblemente con fines lucrativos. Este ataque es difícil de detectar en una organización ya que al no haber modificación de datos no se nota ninguna diferencia, lo que sí es de tener en cuenta es que una organización se puede dar cuenta de este ataque en promedio 180 días después del ingreso del atacante.

4.6. Implementación de un SIEM
Se debe realizar inicialmente un análisis de la red de la organización en la cual se debe tener en cuenta los conceptos de correlación y evidencia digital, con este análisis se debe definir el alcance de las aplicaciones y servidores que se tienen y los requerimientos para la gestión centralizada de registros de eventos de seguridad, se debe ejecutar la definición de una infraestructura de software y hardware para la gestión centralizada de registros de eventos de seguridad que soporte los requerimientos definidos.
Por lo general la definición de dicha infraestructura se realiza por medio del diseño de un sistema de centralización que debe cumplir con los requerimientos definidos por la organización. Lo más común es que los requerimientos se clasifiquen en funcionales y no funcionales

4.6.1 Requerimientos Funcionales: son aquellos que definen la interacción entre el sistema y los usuarios u otros sistemas, independiente de su implementación. Cuentan con las siguientes características

4.6.2 Los registros de los eventos: deben quedar en un punto central. Se debe garantizar que los registros de

eventos quedan en un formato estándar para su posible correlación, independientemente del sistema operativo. Es importante que el formato contenga la identificación del sistema que genero el evento, la hora y fecha en la que ocurrió el evento y el detalle de lo sucedido (logon/logoff, accesos súper usuarios, modificaciones por usuarios no autorizados, etc.). Se debe tener en cuenta el protocolo NTP para todos los servidores de la organización, para que coincidan el envió de los eventos con lo sucedido en el servidor que envía el evento.
Debe existir un proceso de reducción de datos para el proceso de correlación mediante la compresión de datos y borrado de duplicados teniendo en cuenta filtrar los datos combinando varios eventos relacionados en uno solo.
Los registros de eventos deben tener algún mecanismo de identificación del sistema que los genero para efectos de su utilización como evidencia digital.

4.6.3 Requerimientos no funcionales: son aquellos eventos que describen aspectos del sistema que son visibles para el usuario, pero no se relacionan de forma directa al comportamiento funcional del sistema, para lo cual se debe utilizar un mecanismo de autenticación con respecto al sistema que los genero, se debe garantizar integridad de la información para poder contar con los eventos como evidencia digital, se debe verificar que el sistema está en buen funcionamiento en el momento en que se generan o modifican los registros, se debe garantizar que los registros tengan acceso en un periodo de tiempo futuro por ejemplo 1 año, lo cual significa capacidad de almacenamiento teniendo en cuenta disponibilidad.

4.6.4 Definición de herramientas utilizadas para el almacenamiento y la configuración de envió de eventos a el SIEM: aparte de los equipos tecnológicos que van a monitorearse se deben contar con las herramientas apropiadas para él envió de logs.

4.6.5 Sincronización de relojes: Para lograr la centralización de los logs y/o eventos de seguridad se debe realizar la sincronización de los tiempos de los dispositivos de red que van a registrar al SIEM (Servidores, Firewalls, Switch, Routers entre otros), se debe seleccionar un servidor de NTP y realizar en este la configuración del NTPd y configurar los dispositivos de red de acuerdo a su sistema operativo para que hagan uso del protocolo NTP.

4.6.6 Conexión SSH sistemas Linux: se debe crear una conexión SSH entre los servidores o dispositivos Linux y Unix que conectaran con el SIEM, esto se realiza estableciendo un túnel por medio de llaves públicas y privadas, esto con el fin de que el establecimiento de comunicación se realice transparentemente entre las maquinas asegurando el proceso de autenticación. Para él envió de eventos se realizará por el protocolo syslog que es lo mismo que habilitar el puerto UDP 514 en la máquina que enviara los eventos.

4.6.7 Conexión credenciales Sistemas Windows: para establecer la conexión entre sistemas Windows y el SIEM se realiza mediante la creación de un usuario exclusivo con permisos de administrador a nivel del LDAP que envié los logs y/o eventos de seguridad al correlacionador ya que los servicios quedan ligados a esta cuenta de usuario, también se puede dejar configurada una cuenta por dispositivo de red en el SIEM aunque este método puede presentar fallas en ocasiones de envió de logs y/o eventos en el caso que las credenciales del dispositivo de red cambien. Para el envió se realizará mediante la activación de la librería eventlog o mediante un agente propio de la herramienta que realizaría la extracción de logs hacia el SIEM.
Envió logs aplicaciones: se debe garantizar que las aplicaciones que enviaran eventos lo realicen mediante el protocolo syslog o en su defecto por medio del agente o librería configurada por la herramienta SIEM para la recepción de eventos.

4.6.8 Instalación y creación de repositorios de datos: para el almacenamiento de los logs se tienen dos opciones almacenamiento en bases de datos o almacenamientos de logs en archivos planos.

4.6.9 Procedimiento de copias de respaldo: una vez configurado y probado el transporte y el almacenamiento centralizado de los registros de seguridad es necesario realizar una revisión de los procedimientos de elaboración de copias de respaldo. Se debe evaluar si el procedimiento realizado permite periódicamente almacenar las copias tanto en Base de datos, archivo plano o según lo defina la organización, como ya se había indicado las copias de respaldo deben poderse consultar en tiempo presente y futuro.

5. CONCLUSIONES

En el documento pretende dar una guía básica sobre la importancia de la gestión centralizada de registros de eventos de seguridad en una organización; Empezando primero por los conocimientos básicos de que es un SIEM y explicando cada uno de los actores que intervienen en cada una de las etapas tanto en la configuración como en las herramientas que se deben configurar para el correcto envió de logs o evidencias como la forma en la que se debe recolectar y almacenar la información recibida, teniendo en cuenta su integridad y disponibilidad.
Es de tener en cuenta que la centralización de eventos de seguridad es un tema importante ante auditorias ya que facilita la gestión de registros de los eventos de seguridad, ayuda a ahorrar costos y tiempos.
Es importante anotar que la recolección de los sistemas Linux o Unix es más fácil con el protocolo syslog mientras que para sistemas Windows se debe evaluar la herramienta con la cual se van a recolectar los logs si es por agente o activación de alguna librería en especial.
La ingeniería social no tiene que ver nada con la recolección de logs en el SIEM, pero se puede dar el caso que por

ingeniería social se realicen modificaciones en el funcionamiento de recolección de logs y eventos de seguridad del correlacionador.

REFERENCIAS

[1]TORRES, Juan Carlos. RONDÓN, Richard García. "Control, Administración E Integridad De Logs". http://www.criptored.upm.es/guiateoria/gt_m248html

[2] R. GERHARDS (marzo de 2009). «The Syslog Protocol». IETF (Network Working Group), https://tools.ietf.org/html/rfc5424

[3] Comportamiento de la industria cafetera colombiana 2015, (2016), pág:11. Disponible en: https://www.federaciondecafeteros.org/static/files/Informe_Comportamiento_de_la_Industria_2015.pdf

[4]CALDWELL,Mathew. "The importance of Event Correlation for Effective Security Management",ISACA, 2002. https://www.isaca.org/

[5]LIU, Lilia, Análisis forense digital: Un proceso post-morten, IX congreso ISACA Costa Rica 2016,2016, enero de 2018, www.isaca.org/chapters12/costa-rica/events/Documents/Presentaciones_congreso_Isaca 2016/4. Análisis forense digital.pdf.

[6] Superintendecia de Industria y Comercio, Ley 446 de julio de 1998, http://www.sic.gov.co/Normatividad/Leyes/Ley%20446-98.php, marzo de 2018.

[7] LEÓN Ricardo Oliva y SONSOLES Valero Barceló (Coords.), La prueba electrónica validez y eficacia procesal, 1º edición - septiembre de 2016, Ed Juristas con Futuro, pag 23 Colombia co.pool.ntp.org http://www.pool.ntp.org/join.html, The Network Time Protocol Project, 20 Abril 2018

[8] Colombia – co.pool.ntp.org http://www.pool.ntp.org/join.html, The Network Time Protocol Project, 20 Abril 2018.

Juan Combita

Tecnólogo en Análisis y Desarrollo de Sistemas de Información del SENA año 2006, Ingeniero Informático egresado de la Universidad Santo Tomas año 2013, actualmente culminando Especialización en Seguridad Informática.